Claims

1. (previously presented) A method for implementing an intrusion detection system in a network, comprising:

receiving a request at a software agent program to initiate intrusion detection services on a remote computer, wherein the request is issued in response to a notification of a network intrusion;

installing intrusion detection software on said remote computer via said software agent program; and

executing said intrusion detection software on said remote computer via said software agent program.

2. (original) The method of claim 1 further comprising:

receiving a request to terminate intrusion detection services at said software agent program.

3. (original) The method of claim 2 further comprising:

monitoring for fulfillment of a stop condition.

4. (original) The method of claim 3 wherein said stop condition is based on network traffic conditions.

5. (original) The method of claim 3 wherein said stop condition is an expiration time.

6. (cancelled)

7. (previously presented) The method of claim 1, further comprising the step of:

selecting said remote computer from a plurality of eligible computers.

8. (original) The method of claim 7 wherein said selecting step is accomplished based on a network map.

9. (original) The method of claim 7 wherein said selecting step is accomplished based on a knowledge base.

10. (original) The method of claim 1 wherein said request is verified using a cryptographic authentication scheme.

11. (original) The method of claim 1 wherein said request includes a stop condition indicating when to stop executing the intrusion detection software.

12. (original) The method of claim 11 wherein said stop condition is an expiration time.

13. (original) The method of claim 11 wherein said stop condition is based on network traffic conditions.

14. (original) The method of claim 7 wherein said request is verified using a cryptographic authentication scheme.

15. (currently amended) A method for implementing an intrusion detection system on a computer connected to a network, comprising:

receiving a request to become an intrusion detection platform from a remote network location, wherein the request is issued in response to a notification of a network intrusion; and

executing ~~said~~ intrusion detection software in response to the request.

16. (currently amended) The method of claim 15 further comprising:

installing the intrusion detection software on said computer.

17. (original) The method of claim 15 wherein said request includes a stop condition indicating when to stop executing the intrusion detection software.

18. (original) The method of claim 17 wherein said stop condition is an expiration time.

19. (original) The method of claim 17 wherein said stop condition is based on network traffic conditions.

20. (original) The method of claim 17 further comprising the step of:

when said stop condition is fulfilled, ceasing execution of said intrusion detection software.

21. (original) The method of claim 20 wherein said request is verified using a cryptographic authentication scheme.

22. (original) The method of claim 20 further comprising the step of

when said intrusion detection software has ceased executing, un-installing said intrusion detection software.

23. (previously presented) A system for detecting intrusions in a computer network comprising:

a plurality of computers executing software agents;

an intrusion detection server; and

a database configured to store at least one rule defining at least one response to a network intrusion, wherein said intrusion detection server sends a request to execute intrusion detection software to a software agent at at least one of said plurality of computers when intrusion detection services are needed based on the at least one rule stored in said database.

24. (original) The system of claim 23 wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected.

25. (original) The system of claim 23 wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes.

26. (original) The system of claim 23 wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software depending on the time of day.

27. (original) The system of claim 23 wherein said database contains information about the plurality of computers.

28. (original) The system of claim 27 wherein said information includes a map of said computer network.

29. (original) The system of claim 23 wherein said database contains a knowledge base.

30. (previously presented) An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to perform network intrusion detection, said steps comprising:

receiving notification of a network intrusion; and;

installing intrusion detection software on a remote computer via a software agent program in response to the received notification.

31. (cancelled)

32. (currently amended) The article of manufacture of claim 30 ~~31~~ further comprising the step of selecting said remote computer from a plurality of eligible computers.

33. (original) The article of manufacture of claim 32 wherein said selecting step is accomplished based on a network map.

34. (original) The article of manufacture of claim 32 wherein said selecting step is accomplished based on a knowledge base.

35. (original) The article of manufacture of claim 30 wherein said request is verified using a cryptographic authentication scheme.

36. (original) The article of manufacture of claim 30 wherein said request includes a stop condition indicating when to stop executing the intrusion detection software.

37. (original) The article of manufacture of claim 36 wherein said stop condition is an expiration time.

38. (original) The article of manufacture of claim 36 wherein said stop condition is based on network traffic conditions.